Homeland Security Affairs

Volume I, Issue 2 2005 *Article 1*

2005

Potholes and Detours in the Road to Critical Infrastructure Protection Policy

Ted G. Lewis* Rudy Darken†

*Naval Postgraduate School, tlewis@nps.edu

†Naval Postgraduate School, darken@nps.edu

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2005		**00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Potholes and Detours in the Road to Critical Infrastructure Protection Policy	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School ,Center for Homeland Defense and Security,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**14**	

Potholes and Detours in the Road to Critical Infrastructure Protection Policy

Ted G. Lewis Ph.D. and Rudy Darken D.Sc.

Abstract

The national strategy for the protection of critical infrastructure and key assets is not working due to a number of failed strategies, which this article examines in detail: federalism (separation of state and federal governmental controls) advocates that the first line of defense is local first responders; two years after the creation of the Department of Homeland security, and the consequent requirement that states perform vulnerability and risk analysis on their critical infrastructures, DHS has yet to define basic terminology needed for states to perform meaningful analysis ("vulnerability" "risk"), or precisely state the objectives of such analysis; private ownership of the majority of infrastructure assets has been used as an excuse to do nothing – a major myth that is not only wasteful of effort, but dangerous to the security of the nation; and finally, the notion that critical infrastructure sectors are so large and complex that only the highest-consequence, lowest-probability events can be prevented has led to further missteps in the road to critical infrastructure protection policy. This article ends with recommendations for policy changes that address these issues.

AUTHOR BIOGRAPHY: Ted G. Lewis, Ph.D. is Professor of Computer Science at the Naval Postgraduate School and Academic Associate of the Homeland Defense and Security Master Degree program. He has 40 years of experience in academic, industrial, and advisory capacities ranging from an academic career since 1971 at the University of Missouri-Rolla, University of Louisiana, and Oregon State University, to Senior Vice President of Eastman Kodak Company, CEO and President of DaimlerChrysler Research and Technology, North America. Lewis has published over 30 books and 100 research papers, and is the author of the forthcoming book, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation,* to be published by John Wiley & Sons, 2006.

Rudy Darken is an Associate Professor of Computer Science and the Director of the Modeling, Virtual Environments, and Simulation (MOVES) Institute at the Naval Postgraduate School in Monterey, California. Darken also directs modeling and simulation efforts for the Center for Homeland Defense and Security and serves as a Senior Editor of PRESENCE Journal, the MIT Press journal of teleoperators and virtual environments. He holds Master and Doctorate degrees in Computer Science from George Washington University.

KEYWORDS: Critical Infrastructure Protection, risk analysis, public-private partnership, critical infrastructure policy

INTRODUCTION

One can frame the policies of the current national strategy for critical infrastructure protection using a number of colorful analogs, but transportation seems the most fitting because transportation is one of the sectors identified by the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, published by the White House in 2003.[1] Beneath the title of this article is the reality that we have a long way to go to protect critical infrastructure assets – across all sectors – at even modest levels of security. Indeed, if a 1,000-mile journey begins with a single step along a well-defined road, then the national strategy road is badly in need of repairs.

This paper exposes only a handful of the many myths, fallacies, and roadblocks preventing the nation from protecting its second-most important assets: the water, power, energy, telecommunications, information, and transportation systems that make up critical infrastructure (CI).[2] We claim that the first step in this 1,000-mile journey is to fix the potholes and eliminate the detours promoted by the current strategy for protection of the country's CI. To do so, we must understand how the national strategy fails to address reality. We couch these realities in metaphorical terms – as potholes and detours on the road to protecting the nation's critical infrastructures. The term "pothole" is used to identify problems and barriers to making progress, and the term "detour" is used to expose wrong-headed myths, distractions, and bumps in the road to better infrastructure security.

This paper argues against a purely federalist approach to critical infrastructure protection and instead advocates that the federal government take greater responsibility (and control) over state and local decisions; it argues that the first step in this transformation is to set standards, beginning with concise and clear definitions of vulnerability and risk. We then turn to the arguments preventing action – specifically that government is helpless to correct security problems in critical infrastructure because most infrastructures are owned and operated by the private sector. Finally, we make four concrete recommendations on how to improve critical infrastructure protection through re-thinking and re-aligning current policies.

Think Globally, Act Locally

The national strategy is based on the idea that the federal government should set goals and policies, while the states should assume primary responsibility for homeland security, because incidents happen at the local level. Specifically, the National Strategy defines the relationship between federal and state/local governments as follows:

> In addition to securing federally owned and operated infrastructures and assets, the role of the federal lead departments and agencies is to assist state and local governments and private-sector partners in their efforts to:
>
> - Organize and conduct protection and continuity of government and operations planning, and elevate awareness and understanding of threats and vulnerabilities to their critical facilities, systems, and functions;
> - Identify and promote effective sector-specific protection practices and methodologies; and

- Expand voluntary security-related information sharing among private entities within the sector, as well as between government and private entities.[3]

Basically, the federal government is primed to assist state and local governments, but the state/local governments are responsible for implementation of "protection practices, and methodologies." This strategy has a number of deficiencies as pointed out by the first pothole.

Pothole 1: CIP (Critical Infrastructure Protection) is a local problem and therefore the federal government should provide guidance and funding, but state and local jurisdictions must become the first line of defense against attacks on critical infrastructure assets.

This policy is not only dangerous – because local jurisdictions will never have the capability to protect their critical infrastructure assets – but an unfortunate waste of money. In fact, the Government Accounting Office recognized this problem soon after the Department of Homeland Security (DHS) was formed: "The challenges posed in strengthening homeland security exceed the capacity and authority of any one level of government."[4]

Consider the case of the Alaskan telecommunications sector. Alaska's telecommunication infrastructure supports local police, fire, and emergency management functions as well as consumer telephone and Internet access. Without it, Alaskans would be isolated from the rest of the United States. Naturally, it makes sense for the Federal government – through the Department of Homeland Security – to provide funding and training to Alaskans so they can strengthen their telecommunications infrastructure and harden it against potential terrorist attacks. However, this strategy is inadequate and dangerous, because Alaska's telephone and most Internet services are dependent on a single building in Seattle! The Weston building in Seattle is the sixth largest telecom hotel in the nation, and it provides connectivity to the citizens of Alaska. Alaskan's cannot protect this major asset no mater how much money the Federal Government provides, because it lies outside of their jurisdiction.

In addition to the problem of an asset in one state being critical to another state, there is the overarching problem of Interstate Commerce laws that regulate and shape infrastructures such as telecommunications, energy, power, and transportation. States have little power over the Federal regulators when it comes to passing laws that might affect an element of one of these infrastructures and weaken the same infrastructure at the national level. Examples of this can be found in cross-sector interdependencies. For example, the largest electrical power plant in Missouri (New Madrid) is totally dependent on the rail system that delivers coal from Wyoming. Rail transportation and electrical power sectors are regulated by federal agencies – not Wyoming and Missouri – and yet, a policy that may ensure reliable electric power generation in Missouri could conflict with energy policies affecting Wyoming. For example, should Interstate Commerce regulation of Wyoming rail shipments of coal be implemented to raise money to harden the rail transportation system across the USA, the rate payers in Missouri (and other states) would be negatively impacted. There is nothing that the state and local governments can do to offset federal regulation of infrastructure industries.

What should be done to circumvent this pothole? The current strategy is a detour headed in the wrong direction:

Detour 1.1: Allocation of funding for CIP needs to be decided at the state and local level, not the national level.

The problem with this detour is simply the fact that what is critical to a state may not be critical to the nation. Separate funding of State and local districts is a waste of money in most cases because the funding does not address the true need – typically because states and cities do not have the expertise to evaluate risk. Two years after receiving funding from the Department of Homeland Security, most local governments have not spent most of their allocation. It isn't that they can't spend the funds, but rather that there are many restrictions placed by the federal government on the spending of these funds and, most importantly, there is no coherent linkage of these restrictions to an infrastructure resiliency plan. Americans want to know how they are safer because of this funding. There is no answer, but there needs to be one.

Once again, we can use Alaska as an example. The largest nuclear power plant in the nation is located in Arizona, but most of the power consumed by Alaskans comes from a much smaller power plant in Beluga Bay, Alaska.[5] If we use size as a measure of criticality, then it makes more sense to harden the Palo Verde Power Plant in Arizona than the much smaller Beluga Power Plant in Alaska. The problem with this strategy from a national CIP perspective is that the Beluga plant is more important than the Palo Verde plant, because it supplies 60% of all Alaskan power, while the Arizona nuclear power plant supplies less than 3% of the power consumed by the Western Power Grid. If the nuclear plant shut down, it would not be missed, because the Western Grid obtains power from many sources. This is not the case with the Beluga plant. If it fails, most Alaskans will be left without power. Therefore, the Beluga plant is much more critical – to the Western Grid as well as to Alaska – than the much larger plant in Arizona. Size is not always the best measure of criticality.

Detour 1.2: Allocation of funding resources should be based on population, size of state, and other political factors as determined by the Department of Homeland Security.

According to Citizens Against Government Waste, "Funding ratios guarantee each state .75 percent of the funds available for homeland security. This formula initially distributes 40 percent of the funds among the states, with 60 percent for other allocations. Under this model, for example, California, a target-rich state containing 12 percent of the nation's population, received only 7.95 percent of general grants. On the other hand, Wyoming, which received .85 percent of the funds, holds only .17 percent of the population. That means Congress provided $5.03 per capita for California and $37.94 per capita for Wyoming. Similarly, data from the Public Policy Institute of California revealed that Alaska received an astonishing $58 per resident and New York got less than $25."[6]

Once again, allocation of funding based on arbitrary or political considerations will not solve the problem of enhancing security. Instead, it is wasteful and increases the probability of a successful terrorist attack. A national perspective is needed in this risk analysis process as demonstrated by both of these examples. This would reorient funding towards allocation on the basis of risk reduction – hopefully where it can reduce risk the most.

These examples illustrate why the National Strategy's pressure to push responsibility for the protection of critical infrastructures down to the local level is flawed. States and local governments are often not in control of the critical infrastructure assets they depend on. Further, local analysis of local assets results in wasted funding. Arizona is likely to be concerned for its Palo Verde Power Plant when, in fact, the Alaskan power plant at Beluga Bay is more important. But Arizona is unlikely to transfer funding from Arizona to Alaska! These are only the top-level challenges facing the nation – there are several other significant problems lurking at a deeper level.

A Failure to Communicate

One of the most difficult challenges facing the field of critical infrastructure protection is the lack of shared terminology. There are too many people using too many ill-defined terms for the community of homeland security experts to communicate, properly. The lack of widely accepted definitions of terms used in homeland security leads to reinvention of the wheel, false starts, and more detours.

Pothole 2: There are as many definitions of "vulnerability" and "risk" as there are agencies in federal, state, and local governments, combined! Before we can take the first step in a 1,000-mile journey, we need a compass. Currently, there is no universally accepted definition of the most basic measures of criticality – *vulnerability* and *risk*.

For example, the intelligence community typically defines "risk" as R = T + V (Threat plus Vulnerability). The FBI says "risk" is R = I * T * V (probability of an incident times threat times vulnerability).[7] A number of other methodologies use arbitrary metrics to gauge risk. The most popular method of gauging criticality of an asset such as a port, telecommunications center, water treatment plant, or transportation terminal is to assign numbers to each asset and then add them together. In ranked ordering systems such as the U.S. Coast Guard's port security and risk assessment tool, risk is computed by summing assigned numbers to various properties such as damage, casualties, vulnerability, and threat. These numbers are provided by subject matter experts who, in turn, rely on their individual judgment when rating "vulnerability" and "risk." The port asset with the highest total is declared the most critical.

The validity of this approach relies on subject matter experts, which does not address the problem of inconsistency across experts. This leads to uneven ranking, because every expert has a different idea of how to assign numbers. It also leads to meaningless totals, because of the different interpretations of what the numbers mean.

The intelligence community's risk equation is difficult to apply because it is not clear how one compares a low-threat, high-vulnerability asset with a high-threat, low-vulnerability asset. If we add threat and vulnerability together and get the same total, what is the difference? Clearly, a high-threat condition deserves closer scrutiny than a low-threat condition, regardless of the vulnerability, and yet R = T + V produces indistinguishable totals.

The FBI metric cannot deal with combination incidents such as the 9/11 attacks on the World Trade Center and the Pentagon. What does risk mean when the attackers target two or three assets at once? The U.S. Coast Guard metric has no equivalent in the real world, because the numbers are without units. For example, the USCG ranking does not

measure risk in dollars, casualties, or probability. Hence, it cannot be standardized, so how do we compare the results obtained by assessing two different ports?

We need a standard, scientifically exact method of assessing vulnerability and risk. Only then will we be able to define vulnerability and risk. A standard definition means that states and localities will be able to compare apples to oranges, and that the result of vulnerability analysis will mean something – across the 50 states. We can even go further: we can fund projects in a meaningful and productive manner.

Detour 2.1: Individual cities, states, and regions are in the best position to make their own definitions of "vulnerability" and "risk", without the interference of the federal government.

This approach pretty much sums up the current state of affairs. While the DHS has provided general guidelines, each state is left to its own devices when it comes to defining what is critical, and how each defines "vulnerability" and "risk." In 2003, the first year all states were required to perform a complete vulnerability analysis in order to receive federal funding for CIP, the results were meaningless, because every state used a different method, with a different outcome. If was impossible to compare the risk assigned to a bridge, say, in California, with a bridge in Wisconsin.

The definition and terminology problem can be easily solved by establishing simple, yet scientifically valid, definitions. Suppose for example, "vulnerability" is defined as the *probability that an attack will succeed* and "risk" is defined as the *expected value of the damage caused by a successful attack*. Vulnerability is a probability (a number from zero to 100%) and risk is a cost (a number that represents the impact of an attack on an asset or entire sector). Mathematically, risk is V * D, where V = vulnerability and D is typically in units of dollars, casualties, or some other loss.

These definitions are easily applied to all kinds of critical infrastructure assets and they have meaning in the real world; probability and dollars are real-world metrics. Vulnerability is equivalent to 'likelihood', and risk is equivalent to the real-world cost associated with an incident.[8]

Now we can standardize the results so that an assessment made by one expert is identical to an assessment made by another expert. We can compare apples to oranges, and then make progress towards hardening the most critical assets: the higher the risk, the higher the criticality of an asset.

Vulnerability is relative to the threat; e.g. the vulnerability of the Federal Reserve Bank in Manhattan might be 10% relative to a car bomb, and 60% relative to a cyber intrusion. This means there is a 10% likelihood that a car bomb will do enough damage to close the bank and a 60% chance that a cyber attack will halt banking business. Therefore, our definition incorporates the threat as well as the weakness of an asset to a specific threat. A bank may be vulnerable to a cyber attack, but not so vulnerable to a car bomb attack.

Vulnerability is not risk, and risk is not vulnerability. Instead, risk is the product of vulnerability times damage: R = V * D. Risk can be measured in casualties, loss of equipment, financial loss, etc. But you can't mix metrics in one analysis. If you use dollars you can't switch to casualties. The important distinction is that "vulnerability" is the probability of a successful attack, and "risk" is the expected value of damage due to the attack.

Suppose the estimated damage of a successful car bomb attack on the bank is ten million dollars and the cyber attack, one million. Since risk equals vulnerability times damage, the risk associated with a car bombing is one million dollars (10% of $10 million), and the risk associated with a cyber attack is $600 thousand (60% of $1 million). In tabular form, we have the following:

Threat	Vulnerability	Damage	Risk
Bomb	10%	$10 million	$1 million
Cyber	60%	$1 million	$600 thousand

Notice that the bank is more vulnerable to a cyber attack (60%), but the risk of a bombing is higher (one million dollars vs. $600,000)! Risk and vulnerability represent different measures of "criticality." In this case, the cyber threat is "more critical" because the bank has greater vulnerability to a cyber attack, but the bomb is "more critical" because the bank has higher risk to a bombing. It is important to distinguish between vulnerability and risk, because they can produce different definitions of criticality depending on their relative size. Vulnerability is not the same as risk, which means we must decide which is more important – to minimize risk or vulnerability.

What is the most likely incident in the foregoing example? Is it more likely that the bank will suffer a bomb attack or a cyber attack? How do we decide? In most risk assessment methods there is no way to model all possible incidents or events. In this example, the most likely event is a cyber attack (54%), and the least likely incident is a car bomb attack (4%). In addition, there is a 6% probability that both attacks will occur! In other words, the assessment must consider all possibilities. Most risk assessments ignore the likelihood of multiple, simultaneous attacks. The attacks of 9/11 were multiple, simultaneous attacks overlooked by the intelligence analysts, perhaps because their methodology ignored combination events. In our simple car bomb versus cyber attack example, there are actually three threats as summarized below.

Threat	Vulnerability	Damage	Risk
Bomb	10%	$10 million	$1 million
Cyber	60%	$1 million	$600 thousand
Both	6%	$11 million	$1.6 million

Vulnerability and risk assessments must incorporate combination events such that they can be compared across sectors, jurisdictions, and agencies. One way to do this is to standardize the multiple-event model. For example, a rigorous and standard method used in reliability engineering is *fault tree analysis*. Unlike current techniques in use by critical infrastructure protection analysts, fault tree analysis reveals all possible combinations of events, and assigns each a likelihood and risk value. Fault tree analysis can then determine the best allocation of funds to minimize vulnerability or risk. Fault tree modeling is beyond the scope of this article, but it is an established technique, so why not adopt it?

Without a scientific definition of vulnerability and risk, there is no way to perform meaningful risk assessments. There is no way to compare the risk of losing the Palo Verde nuclear power plant with losing the Beluga power plant, and there is no way to decide how much money to spend on prevention of a car bomb attack versus prevention of a cyber attack against banks and government buildings. Existing risk assessment

techniques cannot compare apples to oranges, and when they derive a figure of merit, the numbers are meaningless because they are based on opinion, not scientific measurement.

The "Do-Nothing Policy"

One of the myths circulating among policy-makers suggests that local government is helpless when it comes to CIP, because most critical infrastructure assets are owned and operated by private companies that make up the private sector. How can government protect assets they do not own? The problem with this myth is that it leads to a 'do-nothing" policy. This assumption that private-sector infrastructures are beyond the reach of government agencies is not only wrong, but also dangerous, because it leaves the most critical of assets unprotected.

Pothole 3: Private companies own and operate most critical infrastructure, hence government cannot intervene on behalf of public safety. These owners and operators must provide critical infrastructure protection – not the government. However, because prevention is costly, the owners are unlikely to spend the money needed to protect these assets on behalf of the public they serve.

For example, the Congressional Budget Office states, in an introductory comment to "Why the Private Sector Might Spend Too Little on Security,"

> Businesses would be inclined to spend less on security than might be appropriate for the nation as a whole if they faced losses from an attack that would be less than the overall losses for society. A number of common circumstances can exist in private industry in which there is a gap between the private and public costs of a terrorism event."[9]

This is one of the most prevalent misconceptions in critical infrastructure protection literature. It ignores the burdensome regulation that controls these industries. Most power, telecommunication, and energy companies have little control over their business because of inter-state commerce law and a long history of government regulation. The government still "runs" these sectors through extensive regulation. In nearly every case, these industries fall under inter-state commerce laws or regulation by various governmental agencies designated by the U.S. Congress as overlords. In the electrical power sector, for example, Congress exercises its control through the FERC (Federal Energy Regulatory Commission) and in the telecommunications sector, Congress exercises control through the FCC (Federal Communications Commission). In other words, most critical infrastructure is controlled by the federal government, which dictates how each sector operates.

Let us take the telecommunications sector as an illustrative example. The telecom industry was recently re-regulated by passage of the Telecommunications Act of 1996. This act reasserted detailed governmental control over this vast infrastructure. For example, telecommunications companies like AT&T, Verizon, and Nextel paid billions of dollars in license fees to the US Government for the right to "broadcast" cellular telephone signals through the air. Furthermore, state governments can set prices on telephone service, which leaves very little room for profit. The exercise of this federally and state-centered power suggests the opposite – that government does indeed exercise control over these sectors. In reality, government has the power to protect most critical

infrastructure sectors through existing regulatory agencies. For example, DOE (Department of Energy) sets standards of safety and security for all nuclear power plants; similar regulations control the safety and security of the nation's energy pipelines through the Department of Transportation's Office of Pipeline safety.

The current policy of the Department of Homeland Security appears to be "hands-off" when it comes to dictating security standards in the telecommunications industry. This does not make sense when, in fact, the telecommunications industry is already heavily regulated by federal and state governments. Because the telecommunications business is an inter-state commerce business, there is virtually nothing preventing the addition of security standards to inter-state commerce policy. Indeed, the security standards of sister industries such as the electrical power industry, are dictated by federally run agencies such as the Department of Energy, FERC, and NERC (North America Energy Reliability Council). What prevents implementation of security measures in the telecommunications industry? It is certainly not the case that the telecommunications sector is owned and operated by the private sector.

Detour 3.1: Critical Infrastructure Protection is too expensive to be provided by the companies that own and operate the CI, so we must increase taxes and provide financial incentives to the owners so they will harden their assets in the best interest of the country.

This myth is also widely believed by politicians and policy-makers, but once again, it defies logic and is dangerous because it distracts us from the task at hand – hardening the most critical assets in the various national infrastructure sectors. The first observation is this: most sectors bill consumers proportionally to services or products consumed. The electrical power companies bill by the kilowatt; the telecommunications industry bills by the minute; and the energy sector bills by the amount of energy consumed. In other words, these companies stop making money when services or consumables cease to flow. Continuity of operations already has its own built-in motive – the more reliable the operation, the more money received. Therefore, utility companies are motivated to increase continuity of operations. They do not need governmental incentives to reward them for doing what they do best: deliver services and consumables to the public.

The only thing more expensive than critical infrastructure protection is loss of continuity of operations. The notion that these industries will not protect the sources of their profit is a detour in the road to critical infrastructure protection. Instead of doing nothing, the national policy should be focused on solving the problem of continuity of operations and let the private sector pay for it, because they seek maximal profit. The profit motive works – it is maximized when the sector is operational 100% of the time.

And yet it cost something to harden critical infrastructure assets such as power plants, roads, and railways. Doesn't this cost reduce corporate profits? We only need to look at the immediate past to show how the profit motive works in favor of private sector investment in security. Hurricane Katrina not only damaged much of the infrastructure of New Orleans, it also forced Entergy (the regional power company) to the brink of bankruptcy. Entergy lost revenues because its electrical power distribution lines and gas-powered generators were flooded. The cost of stronger levees would have been much less than the loss of the company. But of course, Entergy has no control over levees – the Army Corps of Engineers does!

The Big Bang Strategy

From the very outset, the strategy of the Department of Homeland Security has been to prepare the nation to respond to high-consequence (high damage), low-probability (low vulnerability) events. One of the early critics of the federal government's strategy identified three weaknesses:

1. Domestic preparedness is focused on *highest consequence*, *least-likely* attack, i.e., low-probability, high consequence WMD (Weapons of Mass Destruction) terrorism,
2. It is geared toward *consequences of chemical/biological WMD* attack, because WMD are becoming *more accessible to terrorists*,
3. It is geared toward federal investments at *the state and local level* due to Federalism and the belief that a*ttacks will be local*, not national; the *US is too large* to maintain a national operational capability at the local level; Federalism gives *states extensive rights and responsibilities*; and the *division of labor* across local, state, federal jurisdictions was compatible with the *Stafford Act*.[10]

The problem with this strategy is that state and local governments are woefully unprepared to meet such emergencies. Furthermore, they are unlikely ever to be capable of responding to big bangs such as a dirty bomb, pandemic, or mass transit emergency. The Hurricane Katrina disaster is the latest illustration of local governments being overwhelmed by a high-consequence, low-probability event.

Pothole 4: Critical Infrastructure assets are so vast and geographically dispersed that we can only protect against the highest-consequence, lowest-probability events.

Closer examination of this pothole shows how impractical it is. Consider the case of a smallpox attack launched in a major metropolitan area.[11] Suppose the eight million inhabitants of Manhattan are exposed to smallpox via a scenario similar to the anthrax contamination perpetrated through the U.S. mail in 2002.[12] Smallpox has a three day incubation period, which means vaccination is effective if given within three days of contraction of the virus. Vaccination is a non-trivial medical procedure that requires a trained person to carefully administer fifteen pinpricks to medically screened recipients. Working twenty-four hours per day, it is estimated that 4,000 health care workers would be needed to vaccinate one million people in a timely fashion. In other words, 32,000 workers would be needed to vaccinate all eight million people living and working in Manhattan!

Logistically, this is an impossible situation. The entire state of New York does not have 32,000 health care workers ready to vaccinate eight million people within three days. Where might these 32,000 workers come from? The NYPD (New York Police Department) employees 34,000 workers, so why not turn this problem over to law enforcement? This leads to another detour.

Detour 4.1: Terrorism is a criminal activity and hence its prevention should be left to local law enforcement, fire fighters, and emergency management services.

If terrorism is a criminal activity, then all our problems are solved! There are more than four million law enforcement, public safety, and medical emergency personnel in the

U.S., which makes the combined "EMS community" larger than the sum total of armed forces under the command of the Department of Defense. The problem is, they are dispersed throughout the country and lack the training, equipment, and intelligence information to leverage the entire community of four million "first preventers." They would need to be coordinated at the national level in order to prepare them to respond to a high-consequence, low-probability event. If the strategy is to be prepared for the high-consequence, low-probability event, then preparations must be national, not local. National readiness requires national organization and coordination. The lessons of Hurricane Katrina remind us that state and local preparedness is insufficient when major events occur.

RECOMMENDATIONS

Historically, most critical infrastructure failures have been caused by natural disasters, not terrorists, so why so much emphasis on the war on terrorism? Is terrorism, and critical infrastructure protection in particular, overrated? The answer must be 'no', because of 9/11. Prior to 9/11 the U.S. considered the homeland safe; non-governmental organizations lacked the capacity to reach across the barriers provided by the Atlantic and Pacific oceans. The asymmetric attacks of 9/11 changed our thinking from elimination of the improbable to careful consideration of unlikely high-consequence events. Second, the 9/11 attacks were – among other things – attacks on critical infrastructure. Manhattan, and the twin towers in particular, are the center of banking and finance for the entire country.

If we are to seriously consider critical infrastructure protection as one of the pillars of homeland security, then several policy adjustments will be required. As a start, the Department of Homeland Security must:

1. Establish itself as a security standards setter and enforcer and act quickly to define basic terminology such as 'vulnerability' and 'risk'. In addition, these definitions must be applied uniformly across the nation so that true risk assessment can become a practical means of evaluation and allocation of funds.
2. The national strategy must leverage national assets to the advantage of high-risk areas of the country rather than distribute responsibility to state and local governments. The U.S. already does this in a number of other areas: the FBI is essentially a national police force; the Department of Interior's forest fire fighters are essentially national fire departments; and the National Guard is essentially an interior army. While all of these must remain under civilian control, there is little reason to hold back; use these national resources to protect national assets.
3. The interface between government and private sector companies has long been established by inter-state commerce laws, regulatory agencies, and the utilities that own and operate most critical infrastructure sectors. There is no reason to do nothing. Legislation needs to be enacted to guarantee "target hardening" of the nation's most critical infrastructure assets.
4. Terrorism is not only a criminal activity – it is a military assault on the entire population. Hence, we must disavow the notion that local law enforcement agencies are capable of preventing acts of violence against critical infrastructure assets. An attack on the Weston building telecom hotel located in Seattle is not a criminal

> activity against Seattle, but a military action against the entire country. It must be dealt with as such.

It is time to re-evaluate the national strategy and replace state and local strategies with a national effort. This has been done within the Department of Interior and Forest Service: large forest fires are fought across regional boundaries, largely by a federal force. It has been done to some extent within the food and agriculture sector: FDA regulators work with the private sector to ensure the safety of the food supply. And whether or not we admit it, the FBI is a national police force that transcends state and local borders.

---

[1] *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Feb. 2003, Department of Homeland Security. http://www.whitehouse.gov/pcipb/physical.html

[2] The most important asset is people – our citizens rank the highest in priority.

[3] *The National Strategy.*

[4] "Homeland Security: Reforming Federal Grants to Better Meet Outstanding Needs," GAO-03-1146T, September 03, 2003.

[5] Arizona's lone nuclear power plant, Palo Verde, ranks second on the Energy Information Administration's (EIA) list of 100 largest electric plants. It is the largest nuclear power plant in the United States. www.eia.doe.gov.

[6] Coulton, Andrew, "DHS Funding Reform Unfinished," December 20, 2004, www.cagw.org

[7] Dean, W., "Risk Assessments and Future Challenges," *FBI Law Enforcement Bulletin,* July 2005.

[8] Lewis, T.G., "Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation" (Wiley: 2006)

[9] Congressional Budget Office, "Homeland Security and the Private Sector," December 2004, Section 3 of 7. www.cbo.gov

[10] Falkenrath: Problems of Preparedness, (Paper 2000-28, Belfer Center, Harvard U.) Dec 2000.

[11] Public Health is one of the critical infrastructure sectors defined by the national strategy.

[12] U.S. Postal Service, "Issues Associated with Anthrax Testing at the Wallingford Facility," GAO-03-787T.